IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 3, March 2017

Study of Alert Correlation Technique

Ankita B. Palekar, Dr. S.S Dhande

Akola, Computer Engineering, Sipna College of Engg & Technology, Amravati, India

Abstract: Alert correlation is a significant technique for arranging large volume of intrusion alerts that are produced by Intrusion Detection Systems (IDSs). The popular trend of research in this area is to drawn out the attack strategies from unprocessed intrusion alerts. The general belief about intrusion detection is that it cannot satisfy the security requirements of organizations. Now, Intrusion response and prevention are becoming very important for preventing the network and removing damage. To launch proper response to stop attacks and prevent them from increasing, it is important to know the real situation of a network and the strategies used by the attackers. This is also the primary aim of using alert correlation technique. However, many of the current alert correlation techniques only focus on grouping inter-connected alerts into different sets without further verifying the strategies of the attackers. The main aim of this paper is to focus on developing a new alert correlation technique that can help to automatically extract attack strategies from a large volume of intrusion alerts, without any prior knowledge about these alerts. The proposed approach is based on two network approaches, namely, Multilayer Perceptron (MLP) and Support Vector Machine (SVM). The output of these two methods is used to verify with which previous alerts, this current alert should be related. This suggests the relationship of two alerts, which is helpful for determining attack scenarios. One of the important features of this technique is that an Alert Correlation Matrix (ACM) is used to store correlation strengths of any two types of alerts. ACM is updated in the training process. The information is then used for drawn out high level of attack strategies.

Keywords: ACE (Alert Correlation Matrix), MLP (Multi-Layer Perceptron), SVM (Support Vector Machine).

I. INTRODUCTION

Recently, attacks on Internet-connected systems have become common & increases rapidly, because of the huge popularity of the Internet and widespread use of automated attack tools.. Not only the number of attacks increased, but the methods used by the attackers are getting more and more complicated. Due to this, security issues have become major factor for many organizations that have networks connected to the Internet. Intrusion detection & alert correlation are the major techniques for preventing information systems. Moreover, it is very hard to define normal behaviour for a system. Even though intrusion detection systems play a very important role in protecting the network, organizations are more interested in preventing intrusion from happening or increasing. However, Understanding the attack pattern & behaviour is a challenging task as the attacker try to change their behaviour in order not to be identified.

However, as intrusion detection systems are increasingly deployed in the network, they could produce large number of alerts with true alerts mixed with false ones. Manually arranging and analyzing these alerts is time-consuming and error-prone. Alert correlation permit for automatic alert clustering, which groups logically interconnected alerts into one groups and allows easy verification of attacks. To launch proper response to stop attacks and prevent them from increasing, it is important to know the real situation of a network and the strategies used by the attackers. This is also the primary aim of using alert correlation technique.

II. RELATED WORK

Alert correlation is the a process of verifying alerts and providing high-level of security to network under surveillance. It contains multiple components. One significant use of alert correlation is to discover the strategies or plans of different intrusions and introduce the aim of attacks. Suppose that the next step of an attacker can be verified by looking at the pattern of the intrusive behaviour, we can take action to prevent the attack from increasing and therefore minimize the harm to the system. Alert correlation provides a means to group which are logically-connected alerts into attack scenarios, it also permits the network administrator to verify the attack strategies. In the past few years, a number of alert correlation techniques have been proposed. Generally, they can be classified into the following types-

- Alert Correlation Based on Known Scenario: In this type of alert, alerts are correlated based on the known attack scenarios. An attack scenario is either learned from training datasets using data mining approach or specified by an attack language. Such approaches can reveal the causal relationship of alerts. This type is restricted to known scenarios.
- Alert Correlation Based on Feature Similarity: In this type of alert, Alerts with higher degree of overall feature similarity will be correlated. This type of alert correlation approaches correlates alert based on the similarities of some selected features, such as source IP address, target IP address, and port number. One of the weakness of this type is that they cannot fully infer the causal relationships between related alerts.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 3, March 2017

- Alert Correlation Based on Prerequisite and Consequence Relationship: This type of approaches are based on the observation that most alerts are not separated, but related to different stages of attacks, with the previous stages preparing for the later ones. Based on this 2 observation, several work is to correlate alerts using prerequisites i.e. required as a prior condition and consequences of corresponding attacks. The requirement of such approaches is specific knowledge about the attacks in order to understand their prerequisites and consequences. Alerts are considered to be correlated by matching the consequences of some previous alerts and the prerequisites of later ones. However, such approaches have one major limitation, that is, they cannot correlate unknown attacks patterns since its prerequisites and consequences are not defined. Even for known attacks, it is very hard to define all prerequisites and all of their possible consequences.

A. Paper Overview

In this paper, we stated a new alert correlation technique that is based on a neural network approach. The unique feature of this approach is that it uses a learning method to get knowledge from the training examples. Once trained, the correlation engine can analyze the probability that two alerts should be correlated. Assigning correlation probability can help to build alert and attack graphs that presents the real attack scenario. In this paper we also introduce an Alert Correlation Matrix (ACM) that can encode correlation knowledge such as correlation strength and average time interval between two types of alerts.

This knowledge is taken during the training process and is used by correlation engine to correlate future alerts. And besides, various attack graphs can be produced out of the ACM, which can help to security analyst to study the strategies or plans of attackers. One other advantage of using ACM is that it is periodically updated after the training process, which enables it to infer the changes in the existing attack patterns or the newly produced patterns. The ACM is proved to be operative for enhancing the alert graph generation. The rest of this paper is organized as follows. Section 2 provides Proposed Alert Correlation Techniques for Extracting Attack Strategy. Under this section we completed the overview of attack strategies, ACM, feature selection; alert correlation using MLP and SVM. Finally, the conclusions and some suggestions for future work are given in Section 3.

III. PROPOSED ALERT CORRELATION TECHNIQUES FOR EXTRACTING ATTACK STRATEGY

A. Overview

Generally, the attack strategies are represented as attack graphs. Security experts can manually create attack graphs by using knowledge such as topology and vulnerabilities of the protected network. But, this approach is time-conserving and responsible for error. Day-by-day, many alert correlation techniques have been introduced to help security analysts to learn strategies and attack patterns However, all of these approaches have their own boundaries. They either cannot open up the causal relationship among the alerts, or need a huge number of predefined protocols to correlate alerts and produce attack graphs. In this paper, we propose another alert correlation method that hits the production of attack graphs from a huge volume of raw alerts. The proposed correlation concept is depends on multi-layer perception (MLP) and Support Vector Machine (SVM). More importantly, we use the output of MLP or SVM to relate correlated alerts in a way that they represent the corresponding attack scenarios. Here we also reveal an alert correlation matrix into the correlation process. This is basically a knowledge base that encrypts statistical correlation information of alerts. It is possible to infer causal relationship based on this information. The following subsections describe the selection and determine the value of features that are used for alert correlation, and then explain the proposed correlation technique.

B. Alert Correlation Matrix (ACM)

The ACM is proved to be operative for enhancing the alert graph generation. The correlation strength between two types of alert plays an important role in attack pattern analysis. It discovers the causal relationship of the two alerts. However, deciding how strong two alerts are correlated is hard because it needs huge knowledge regarding the attacks and their relations. However, introducing the correlation strength for all of them seems to be impossible. This approach solves the problem of having a huge number of various alerts. But it is insufficient for attack strategy verification and intrusion prediction. The Alert Correlation Matrix (ACM) that is proposed in this paper involves correlation weights between any two alerts, and therefore provides more information for alert correlation and attack strategy determination.

	a1	a2	a3	a4	a5
a1	C(a1,a1)	C(a1,a2)	C(a1,a3)	C(a1,a4)	C(a1,a5)
a2	C(a2,a1)	C(a2,a2)	C(a2,a3)	C(a2,a4)	C(a2,a5)
a3	C(a3,a1)	C(a3,a2)	C(a3,a3)	C(a3,a4)	C(a3,a5)
a4	C(a4,a1)	C(a4,a2)	C(a4,a3)	C(a4,a4)	C(a4,a5)
a5	C(a5,a1)	C(a5,a2)	C(a5,a3)	C(a5,a4)	C(a5,a5)

Fig. 1: Alert Correlation Matrix

Fig.1 shows alert correlation matrix & by using this, we can give the formal definition of ACM as following -

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 3, March 2017

An Alert Correlation Matrix (ACM) for n alerts a1; a2; is a matrix with n * n cells, each of which contains a correlation weight of two types of alert. Figure 1 shows an ACM example of five alerts a1; a2; a3; a4,and a5. We use C(ai; aj) to denote a cell in ACM for alerts ai and aj . Note that the ACM is unsymmetrical. It encrypts not perpetual relation between two alerts. As shown in Figure 1, C(a1; a2) and C(a2; a1) represent two various temporal relationships. C(a1; a2) suggests that alert a2 reach after a1, while C(a2; a1) shows that alert a2 reach before a1. These two differing situations helps to understand the relationship of these two types of attacks. Each cell in ACM holds a correlation weight. It is computed as follows:

$$W_{C(a_i,a_j)} = \sum_{k=1}^{N} p_{i,j}(k)$$

N is the number of times these two types of alert have been directly correlated, and p(k) is the probability of the k^{th} correlation. These correlation weights are periodically updated during the training process.

C. Correlation Strength

It is a generalised value between 0 and 1. The more the value is, the stronger the two alerts are correlated, the values on the diagonal represent the strength of the self-correlation. In other words, it indicates that the probability that one type of alert may repeat itself in one scenario. The ACM also encrypt the temporal relationship between two types of alerts. Accordingly, two types of correlation strength are introduced, namely, Backward Correlation Strength and Forward Correlation Strength The reason for having two various types of correlation strength is that, for alert correlation, we are more interested in finding which previous alerts should be correlated with the current one. And for intrusion detection and attack strategy recognition, we are eager to know about what alert is most likely to happen next. Backward and forward correlation strengths are respectively used for those two cases. The calculation of backward correlation strength is basically the generalization of the correlation weight of vertical elements in ACM, while generalizing the correlation weights of horizontal elements gives the forward correlation.

$$\Pi^{f}_{C(a_i,a_j)} = \frac{W_{C(a_i,a_j)}}{\sum_{k=1}^{N} W_{C(a_i,a_k)}}$$

$$\Pi^{b}_{C(a_i,a_j)} = \frac{W_{C(a_i,a_j)}}{\sum_{k=1}^{N} W_{C(a_k,a_j)}}$$

N is the number of times these two types of alert have been directly correlated, and k is the probability correlation.

IV. FEATURE SELECTION

When an intrusion detection system generates an alert, it also gives the information associated with that alert, such as timestamp, source port destination port, source IP address, destination IP address, and type of the attack. All of these can be used to build the features for alert correlation. The scenario presented in this paper is similar to the probabilistic alert correlation technique in a sense that they all include selecting set features, calculating the probability based on these features and deciding if two alerts should be correlated. The important difference between these two scenarios is the way they calculate the probability. For the proposed correlation technique, the following 6 features are selected.

F1: If the two alerts having same target port numbers-

Before an attacker can guess vulnerability of the service that is running on a particular port, he or she must first know if this port is opened. This feature is important for comparing two attacks that attack on the same port. A value 0 or 1 is used to indicate the matched case and unmatched case, respectively.

F2: The resemblance between two source IP addresses of two alerts –

The source IP address can be displayed as the identity of an attacker, in a network-based attack. In some cases, two alerts with same source IP addresses are belong to the same attack scenario and therefore could be compared. The reason is that these two alerts might have been triggered by the harmful behaviour of the same attacker. However, an attacker may use different IP addresses to perform various attacks against the target system or network. Or even worse, the attackers may satire their IP address and then attack the target. Therefore, the source IP address cannot always be used to identify the attacker. This feature indicates that two alerts come from the same attacker and is calculated as follows:

$$sim(ip_1, ip_2) = n/32$$

where n is the maximum number of high order bits that these two IP addresses match and 32 is the number of bits in an IP address. For example:

ip1=192.168.0.001 ⟶ 11000000 10101000 00000000 00000001

ip2=192.168.0.201 ⟶ 11000000 10101000 00000000 10000001

then n = 24 and sim(ip_1; ip_2) = 0.75. This indicates that two IP addresses are from same network and could be used by the same attacker in various stage of an attack.

F3: The similarity between two target IP addresses of two alerts-

The similarity of two target IP addresses is more important than one of two source IP addresses. When two target IP ad- dresses are not the same, in such a case the correlation probability of them is normally less. If two source IP addresses are different, the corresponding two alerts can still have a high chance of correlation. For properly determine these two cases, training patterns should be properly selected.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 3, March 2017

F4: The backward correlation strength between two types of alert -
The value of this feature is between 0 and 1 indicating the backward correlation strength between two types of alert. This knowledge is helpful for deciding whether two alerts are correlated or not. But defining such correlation strength for each pair of alerts is almost not possible. The best way to study such concept is to learn from examples, i.e. use correlation probability to update the correlation strength and correlation weight between two types of alerts.
F5: The frequency that two alerts are correlated -
The value of this feature is between 0 and 1. If the value of F4 is low, it indicates that the corresponding two alerts are rarely correlated, and therefore the backward correlation value is unreliable at this time due to the presence of miscorrelation. When the value of F6 becomes large, it indicates that these two alerts are regularly correlated; the percentage of miscorrelation should be low. If ¦b has been updated many times and becomes "mature", then we can trust because these two types of alert are now statistically correlated.
F6: If the source IP address of the current alert matches the target IP address of a previous alert-
This feature helps to infer that whether or not the source of an alert is the target of a previous alert. We include this feature because in many cases, attackers may compromise a host and use it to attack another target.

V. ALERT CORRELATION USING MLP AND SVM

In this section, alert correlation approach based on MLP and SVM is explained.
Overall, the task of such a technique is to determine:

- Whether or not two alerts should be correlated.
- If yes, the probability with which they are correlated.

If appropriate training data is provided, both MLP and SVM can fulfil these requirements. The correlation probability is required because it is useful for practical recognition cases, and also gives the uncertainty of correlation.

A. Alert Correlation Using Multi-Layer Perceptron

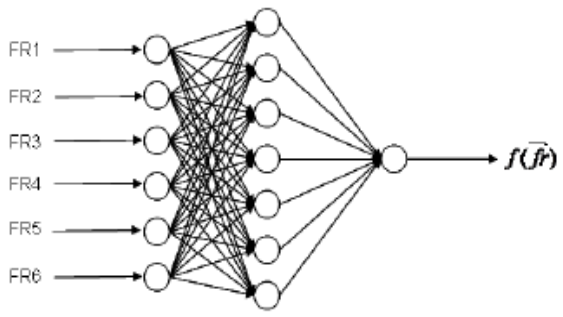

Fig 2: MLP Structure For alert Correlation

Fig.2 shows the MLP structure that is used for alert correlation. It contains six inputs, with seven neurons, and one output. The input is a vector of 6 elements, each of which represents one of the features defined above.

$$\vec{fr} = [F1; F2; F3; F4; F5; F6]$$

The output of this MLP is the value between 0 and 1, indicating the probability that two alerts are correlated.

B. Alert Correlation Using Support Vector Machine

Support Vector Machines (SVM) was first discovered by Vapnik and his co-workers in 1992. It is an implementation of the method for risk minimization. It has been proven to be very robust for pattern classification and nonlinear regression. For given two alerts, we determine if they are correlated or not. This is the main advantage of using SVM for alert correlation.

VI. CONCLUSIONS AND FUTURE WORK

Recently, the research in the alert correlation technique is getting wider because of the fact that generating large number of alerts has become a major problem of traditional IDSs. Alert correlation is an important technique to associate the outputs from many IDSs and provide a high-level of the security to the network. Now-a-days, many correlation approaches have been suggested. However, very few of them provide the capability of automatic extracting attack strategies from alerts.

Most of them simply combine the alerts into various groups. This paper presents an alert correlation technique based on two neural network approaches: Multilayer Perceptron (MLP) and Support Vector Machine (SVM). The aim of the proposed correlation technique is not only to associate alerts together, but also to represent the correlated alerts in a way that they reflect the corresponding attack strategies. The outputs of MLP and SVM are helpful for constructing such attack scenarios. Both MLP and SVM have their own strengths for alert. The use of ACM is also proved to be effective to drawn out high level attack strategies. Attackers often change attack patterns to achieve their goal. For example, they may use various attacks to collect information and compromise the target system to gain root access. For analyst, attack graphs provide useful information to study the variations of attack pattern. Automated analysis techniques on top of attack graphs can greatly reduce the system analyst's workload. Some graph theories can be used to study the similarity of attack graphs, and to know about the similarity of various type of alerts. In this paper we use six features for the alert correlation. MLP and SVM have the capability to handle high dimension input. So, the proposed alert correlation technique can be improved by introducing more features.
Attack graphs enable network analyst to understand the strategies of attackers. In order to prevent the network from various attacks, the analyst will perform risk assessments against the attack strategies. By associating the topology and vulnerability information, it is also possible to determine the victims of a particular attack.

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 3, March 2017

REFERENCES

[1] Njogu,H.W.,jiawei L., Kiere,J.N./& Hanyurwimfura,D.(2013).A comprehensive vulnerability based alert management approach for large networks.
[2] Haukeli,J. (2012). False positive reduction through IDS network awareness.
[3] Gupta,D., Joshi,P.S., Bhattacharjee,A.K., & Mundada, R. S. (2012). IDS alerts claasification using knowledge-based evaluation.
[4] Goodall, J., R., Lutters,W. G. & Komlodi, A. (2009) Developing expertise for network instrusion detection. Information technology & people, 22(2), 92-108. Doi: 10.1108/09593840910962186
[5] Njogu,H.W.,& jiawei, L.(2010). Using Alert Cluster to reduce IDS alerts.
[6] Xiao,M., & Xiao, D.(2007). Alert verification based on attack classification in collaborative instrusion detection.
[7] Bolzoni,D., Crispo,B., Etalle,S. (2007). An architecture for alert verification in network instrusion detection system.
[8] F. Cuppens and A. Miege, Alert correlation in a cooperative intrusion detection framework, Security and Privacy, 2002
[9] F. Cuppens and Rodolphe Ortalo, Lambda: A language to model a database for detection of attacks, Proceedings of Recent Advances in Intrusion Detection, 3rd International Sympo-sium, (RAID 2000) (Toulouse, France) (H. Debar, L. M, and S.F. Wu, eds.), Lecture Notes in Computer Science, Springer-Verlag Heidelberg, October 2000, pp. 197{216.
[10] S.T. Eckmann, G. Vigna, and R.A. Kemmerer, Statl: An attack language for state-based intrusion detection, Proceedings of the 1st ACM Workshop on Intrusion Detection Systems (Athens, Greece), November 2000.
[11] MIT Lincoln Laboratory, 2000 darpa intrusion detection scenario speci¯c data sets, 2000.
[12] Peng Ning, Yun Cui, and Douglas S. Reeves, Constructing attack scenarios through correlation of intrusion alerts, Proceedings of the 9th ACM conference on Computer and communication security (Washington D.C., USA), ACM Press, November 2002, pp. 245{254.
[13] Peng Ning, Yun Cui, Douglas S. Reeves, and Dingbang Xu, Techniques and tools for analyzing intrusion alerts, ACM Transactions on Information and System Security (TISSEC) 7 (2004).